Docket No.: 62807-173 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Koichi TANIMOTO, et al.	:	Confirmation Number: 9181
Serial No.: 10/801,115	:	Group Art Unit: 2131
Filed: March 16, 2004	:	Examiner:

For: VERIFICATION RESULT RECORDING METHOD AND APPARATUS FOR CREATING SIGNATURE VERIFICATION LOG

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

At the time the above application was filed, priority was claimed based on the following application:

Japanese Patent Application No. JP 2004-028794, filed on February 5, 2004.

A copy of each priority application listed above is enclosed.

Respectfully submitted,

MCDERMOTT WILL & EMERY LLP

Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 KEG:gav
Facsimile: (202) 756-8087
Date: July 28, 2004

10/801,115
July 28, 2004

日本国特許庁
JAPAN PATENT OFFICE

McDermott Will & Emery LLP

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed th this Office.

出願年月日
Date of Application: ２００４年　２月　５日

出願番号
Application Number: 特願２００４－０２８７９４

[ST. 10/C]: [ＪＰ２００４－０２８７９４]

願人
Applicant(s): 株式会社日立製作所

２００４年　３月３１日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願
【整理番号】　K03017551A
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　谷本　幸一
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　宮崎　邦彦
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　伊藤　信治
【発明者】
　【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所公共システム事業部内
　【氏名】　大本　周広
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社　日立製作所
【代理人】
　【識別番号】　100075096
　【弁理士】
　【氏名又は名称】　作田　康夫
【選任した代理人】
　【識別番号】　100100310
　【弁理士】
　【氏名又は名称】　井上　学
【国等の委託研究の成果に係る記載事項】　国等の委託研究の成果に係る特許出願（平成１５年度通信・放送機構「次世代証拠基板技術に関する研究開発」委託研究、産業活力再生特別措置法第３０条の適用を受けるもの）
【手数料の表示】
　【予納台帳番号】　013088
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
署名者側装置と、検証者側装置と、公開機関側装置とからなる署名システムにおいて、署名の検証に関わる情報を記録した検証ログを作成する検証結果記録方法であって、
前記署名者側装置は、
作成した署名に関する署名記録を、連鎖関係を伴って署名者側署名履歴として記録し、
前記公開機関側装置は、
前記署名者側装置から預託された前記署名記録を公開し、
預託された複数の署名記録を、連鎖関係を伴って公開機関側署名履歴として記録し、
前記公開機関側署名履歴中の所定の署名記録を新聞公開署名記録として公開し、
前記検証者側装置は、
前記公開機関側署名履歴を用いて、
前記新聞公開署名記録から前記署名者側装置が公開を預託した前記署名記録まで、署名間の連鎖関係の整合性が取れていることを検証し、
前記署名者側署名履歴を用いて、
前記署名者側装置が公開を預託した署名記録から前記検証対象署名に関わる署名記録まで、署名間の連鎖関係の整合性が取れていることを検証し、
前記検証に利用したデータを検証ログとして記録する、
ことを特徴とする検証結果記録方法。
【請求項２】
請求項１記載の検証結果記録方法であって、
前記検証ログに記録される前記検証に利用したデータは、
前記検証対象署名と、
前記署名者側署名履歴と、
前記公開機関側署名履歴と、
前記新聞公開署名記録である、
ことを特徴とする検証結果記録方法。
【請求項３】
請求項２記載の検証結果記録方法であって、
前記検証ログから、前記検証に利用したデータである、前記検証対象署名と、前記署名者側署名履歴と、前記公開機関側署名履歴と、前記新聞公開署名記録とを抽出し、
抽出した前記検証に利用したデータを利用して、前記新聞公開署名記録から前記検証対象署名に関わる署名記録まで、署名間の連鎖関係の整合性が取れていることを検証することにより、検証ログを検証すること
を特徴とする検証結果記録方法。
【請求項４】
署名検証を行う検証者側装置であって、
署名者の公開鍵を用いて検証対象署名の検証を行う受信処理と、
新聞公開署名記録を起点として、前記検証対象署名までの連鎖関係を、署名者側署名履歴と公開機関側署名履歴とを用いて検証する検証処理と、
前記検証処理に利用したデータから検証ログを作成し記録する検証記録保存処理と、を実行する
ことを特徴とする検証者側装置。
【請求項５】
署名の信頼性向上処理を行う公開機関側装置であって、
署名者側装置から預託された署名記録を公開する公開処理と、
前記署名者側装置に署名記録の公開を催促する公開催促処理と、
前記署名者側装置に対して、他の署名者側装置から預託された署名記録を公開したことを通知する公開通知処理と、
前記署名者側装置に代わって、検証対象署名を、検証に必要なデータを収集して検証し

、検証ログを作成して検証結果を通知する検証代行処理と、を実行する
ことを特徴とする公開機関側装置。
【請求項６】
請求項５記載の公開機関側装置であって、
前記公開処理として、
署名者側装置からより公開を預託された署名記録を公開する公開処理と、
公開した前記署名記録に関わる情報を記録する公開情報登録処理と、
公開した前記署名記録に関して、他の署名者側装置から公開通知依頼を受け取っていたかどうかを確認する通知依頼有無確認処理と、
公開した前記署名記録に関して前記公開通知依頼を受け取っていれば、前記他の署名者側装置へ通知する公開通知処理と、を実行する
ことを特徴とする公開機関側装置。
【請求項７】
請求項５記載の公開機関側装置であって、
前記公開催促処理は、
署名記録の公開を催促するべき署名者を特定する対象者抽出処理と、
署名記録の公開を催促する催促文書を前記特定した署名者が利用する署名者側装置に送信する催促書送信処理と、
前記催促文書を送信したことを記録する催促情報登録処理と、
を実行する
ことを特徴とする公開機関側装置。
【請求項８】
請求項５記載の公開機関側装置であって、
前記公開通知処理は、
前記他の署名者側装置から前記公開通知依頼を受け取り、前記公開通知依頼の内容をデータベースに記録する通知依頼内容登録処理と、
前記通知依頼内容を記録した前記データベースから、通知依頼元である前記他の署名者側装置の情報を抽出する通知依頼者抽出処理と、
前記通知依頼元である前記他の署名者側装置に、通知依頼対象署名者による公開署名記録が公開されたことを通知する通知書送信処理と、
を実行する
ことを特徴とする公開機関側装置。
【請求項９】
請求項５記載の公開機関側装置であって、
前記検証代行処理は、
署名者側装置から検証代行の依頼を受け付ける検証代行依頼受取処理と、
検証依頼された検証対象署名について、検証に必要な公開署名記録、署名履歴を収集する検証データ収集処理と、
前記検証データ収集処理によって収集したデータを用いて、検証依頼された前記検証対象署名を検証する署名検証処理と、
前記検証結果、および前記検証に利用したデータを記録した検証ログを作成し、検証依頼元である前記署名者側装置に送付する検証ログ発行処理と、
依頼された前記検証対象署名について、検証状況を前記データベースに記録する検証状況登録処理と、
依頼された前記検証代行処理について、前記検証状況を確認する検証状況確認処理と、
を実行する
ことを特徴とする公開機関側装置。

【書類名】明細書
【発明の名称】署名検証ログを作成する検証結果記録方法とその装置
【技術分野】
【０００１】
本発明は、ディジタル署名技術に関する。
【背景技術】
【０００２】
ディジタル署名（以下、署名という）の証拠性を高める技術として、署名作成の際に、その時点までの署名履歴情報を反映させ、作成した署名に関わる情報を、署名記録として新たに署名履歴に追加する手法がある（例えば、特許文献１または特許文献２参照）。この方法により作成した署名は連鎖構造を持ち、改竄は困難となる。検証の際は、署名に対する検証の他に、連鎖の検証も行うことにより、改竄に対して厳密な検証が行える。この技術は、長期に渡って電子文書の証拠性を維持することを可能にするもので、ヒステリシス署名技術と呼ばれる。
【０００３】
この技術においては、署名の検証を行う場合には、信頼できる署名から連鎖が繋がっている署名は全て信頼できると判断する。連鎖の検証も含めた厳密な署名検証に必要なデータは、検証対象署名、検証対象データ、および署名履歴である。この技術では、過去の署名を記録したこの署名履歴が、証拠性維持のよりどころとなっている。また、連鎖検証の起点となる信頼できる署名を作成するために、署名履歴の一部を第三者機関である公開機関を通じて公開するという方法が考えられている。
【０００４】
【特許文献１】特開２００１－３３１１０４号公報
【０００５】
【特許文献２】特開２００１－３３１１０５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
上記技術において、何らかの理由で署名履歴が失われてしまうと、以前には検証できていた署名の検証も困難となってしまう。従って、過去に少なくとも一度検証できていた署名については、署名履歴が失われたとしてもその証拠性が保証されることが望ましい。
【課題を解決するための手段】
【０００７】
本発明は、過去に検証した署名について、その証拠性を長期に渡って保証する技術を提供する。具体的には、検証の際に検証に利用したデータをログとして残し、それを長期にわたる保証において利用する。
【０００８】
すなわち、本発明は、ヒステリシス署名技術を利用して作成した署名を検証した場合に、検証した署名の証拠性を長期に渡って維持できる検証記録保存機能を提供する。
【０００９】
本発明において、「署名記録」とは、作成あるいは受信した個々の署名から作られる署名情報であり、「署名履歴」とは、複数の「署名記録」が保存されたファイルを指す。また、署名履歴中の署名記録は、所定の間隔を置いて、その時点での最新のものが公開機関を通して、公開され、公開された署名記録は、公開機関によりその信頼性が保証されているものとする。
【００１０】
本発明では、長期経過後のヒステリシス署名技術に基づく署名を検証する際には、署名履歴中の公開機関側装置によって信頼性が保証された署名記録から、検証対象署名の署名記録まで連鎖の整合性が取れているかどうかを検証する。本発明の検証記録保存機能は、検証の際に利用した署名記録、公開機関側装置に公開した署名記録、および検証対象署名

を検証ログに記録する。

【００１１】

これにより、たとえ署名履歴が消われた場合であっても、検証ログを調べることによって、それに記載されている署名の正当性を示すことができる。　検証ログを、消失した場合であっても、再度、署名履歴の検証を行うことによって、検証ログを復元できる。

【００１２】

また、本発明では、署名の信頼性を保証するための公開機関のサービス形態を提供する。すなわち、本発明では、公開機関側装置において、信頼できる署名を確実に作成して、連鎖検証に利用できるように、ユーザの公開忘れを防止するサービスや、ユーザに代わって検証を代行するなど、ユーザの利便性も考慮し、かつ信頼のある検証を行うサービスのための仕組みを提供する。このようなサービスの提供によって、一度検証した署名は、改めて検証することなくその証拠性を長期に渡って示すことができるようになる。

【発明の効果】

【００１３】

本発明によれば、署名履歴などの証拠情報が消失してしまった場合でも、過去の検証時に作成された検証ログを利用して、証拠性を長期に渡って維持することができる。

【発明を実施するための最良の形態】

【００１４】

図１は、本発明を適用した一実施形態におけるヒステリシス署名システムの概略図である。

【００１５】

図示するように、本ヒステリシス署名システムは、署名作成、署名検証、検証記録保存、署名記録の公開を行うユーザ側装置１０１～１０３と、各ユーザから送られてきた署名記録を公開する公開機関側装置１０４とを含んで構成される。ユーザ側装置１０１～１０３と公開機関側装置１０４は、インターネットなどのネットワーク１０５を介して繋がっている。

【００１６】

ユーザ側装置１０１～１０３は、図２に示すように、記憶装置２０２と、ネットワークを介して他の装置と通信を行うための通信装置２０４と、キーボードやマウスなどの入力装置２０５と、ディスプレイなどの表示装置２０６と、ＣＰＵ２０１と、これらを接続するインタフェース２０３とから構成される。

【００１７】

記憶装置２０２には、署名を作成して署名付き文書を送信する送信プログラム２０７と、署名付き文書を受信して署名を検証する受信プログラム２０８と、署名履歴の連鎖検証も含んだ検証を行う文書検証プログラム２０９と、検証した際に検証に使用したデータを検証ログに記録する検証記録保存プログラム２１０と、公開依頼書を作成して公開署名記録を公開機関側装置１０４に送信する公開依頼書送信プログラム２１１と、自分の署名履歴を他のユーザに送信する履歴送信プログラム２１２と、他のユーザから他のユーザの署名履歴を受信する履歴受信プログラム２１３と、署名履歴ファイル（署名履歴という）２１４と、ユーザ情報ファイル２１５と、他ユーザから受信した署名履歴を保存する他ユーザ署名履歴保存ファイル２１６が格納されている。

【００１８】

以下の説明における各プログラム２０７～２１３の処理は、インタフェース２０３を介して呼び出された各プログラムをＣＰＵ２０１が実行することにより、ユーザ側装置１０１～１０３上で実現されるものである。各プログラムは、予め記憶装置２０２に格納されていてもよいし、ユーザ側装置１０１～１０３が利用可能な媒体を介して導入されてもよい。媒体とは、たとえば、公開機関側装置１０４に着脱可能な記憶媒体や、通信装置２０４に接続するネットワークまたはネットワークを伝搬する搬送波といった通信媒体を含む。

【００１９】

また、これらのプログラムは、署名作成時に署名履歴情報を反映させるヒステリシス署名技術を利用している。ユーザ側装置は、署名者のユーザ側装置（以下、署名者側装置という）と検証者のユーザ側装置（以下、検証者側装置という）とに区別される。署名者側装置は署名を作成したユーザ側装置を表し、検証者側装置は、署名を検証するユーザ側装置を表す。ただし、署名者側装置が自分の作成した署名を検証する場合は、署名者側装置と検証者側装置は同一である。

【００２０】

なお、公開機関側装置１０４の構成は、後に図８を用いて説明する。

【００２１】

図３は、署名者のユーザ側装置１０１～１０３が送信文書３０７に対し署名３０８を作成した後、署名付き受信文書３０９を受信し署名検証した場合の署名履歴の様子を示したものである。この場合、ユーザ側装置１０１～１０３は、署名作成時は署名者側装置であり、署名付き文書受信時には、検証者側装置となる。署名作成時には、署名者側装置は、送信プログラム２０７の処理により、送信文書３０７と前回の署名記録３１３のハッシュ値に対して秘密鍵を作用させて署名３０８を作成する。作成後、前回の署名記録３１３と作成した署名３０８から、署名記録３１４を作成し、署名履歴３１１に追加する。

【００２２】

署名受信時には、検証者側装置は、受信プログラム２０８の処理により、受信文書３０９に対する署名３１０を公開鍵を用いて検証する。検証後、前回の署名記録３１４のハッシュ値と署名３１０から署名記録３１５を作成し、署名履歴３１１に追加する。以上のように、署名作成時や署名受信時において、署名情報を記録した署名記録が作られる。前回の署名情報が次回の署名作成に利用されるため、署名間に連鎖関係が生じる。通常の公開鍵を用いた署名検証に加えて、この連鎖関係を検証する(以降、連鎖検証と呼ぶ)ことにより、より確実な署名の検証を行うことができる。

【００２３】

ユーザ側装置１０１～１０３における署名記録は、署名アルゴリズム等の情報を示す「識別番号３０１」、何番目に作られた署名記録であるかを示す「署名番号３０２」、署名作成（送信）時に作成した署名記録か、署名検証（受信）時に作成した署名記録かを表す「種別３０３」、連鎖検証に利用する「前回署名記録のハッシュ値３０４」、署名作成時のみ記録する「署名作成対象文書のハッシュ値（文書のハッシュ値という）３０５」、「署名or受信署名記録情報３０６」（署名作成時は、作成した署名。署名検証時は、受信した署名の署名番号とその署名に対する署名記録のハッシュ値を結合したもの）を含んで構成される。なお、どの署名がどの署名記録中に残っているか判別するために、署名作成時においては、署名履歴に今回新たに追加される署名記録の署名番号を、作成した署名に付加する。作成された署名記録が順に記録されたファイルが署名履歴である。

【００２４】

ユーザ側装置１０１～１０３は、予め定めた規則、たとえば定期的に最新の署名記録を公開機関側装置１０４などの信頼できる第三者機関側装置に預託する。具体的には、公開依頼書送信プログラム２１１の実行により、ユーザ側装置１０１～１０３は自身の署名履歴２１４から最新の署名記録を取得し、その署名記録を含んだ公開依頼書を公開機関側装置１０４に送信する。公開機関側装置１０４側では、受け取ったユーザ側装置１０１～１０３の署名記録を公開する。公開機関側装置１０４に預託され公開された署名記録を預託公開署名記録と呼ぶ。

【００２５】

また、公開機関側装置１０４もヒステリシス署名を利用することで、ユーザの預託公開署名記録の正当性をより一層高めることができる。公開機関側装置１０４の公開の仕組みを図４に示す。

【００２６】

公開機関側装置１０４は、ユーザ側装置１０１～１０３より預託公開署名記録が付加された公開依頼書４０８を受け取ると、公開プログラム８０９の処理により、その公開依頼

書４０８と前回の署名記録４１２のハッシュ値に対して公開機関側装置１０４の秘密鍵を作用させて署名４０９を作成する。

【００２７】

また、その公開依頼書４０８に対して、公開依頼書ごとに決められる固有の公開IDを作成する。そして、作成した署名４０９と公開ID、および預託公開署名記録とから、署名記録４１３を作成し、公開機関側装置１０４の署名履歴４１０に記録する。最後に、預託公開署名記録と公開ID、および公開依頼書送信元のユーザ名（もしくはメールアドレス）とを公開する。

【００２８】

公開先としては、掲載場所が限られる新聞よりは、Webなどが望ましい。公開IDは、公開依頼書ごとに固有であるので、公開IDによって、Webに公開された預託公開署名記録と公開機関側装置１０４の署名記録とを対応付けることができる。

【００２９】

公開機関側装置１０４における署名記録は、署名アルゴリズム等の情報を示す「識別番号４０１」、何番目に作られた署名記録であるかを示す「署名番号４０２」、連鎖検証に利用する「前回署名記録のハッシュ値４０３」、「署名値４０４」、公開依頼書ごとに作成された「公開ID４０５」、公開した預託公開署名記録の署名番号「公開署名記録番号４０６」、公開した預託公開署名記録のハッシュ値「預託公開署名記録のハッシュ値４０７」を含んで構成される。この署名記録が順に記録されたファイルが公開機関側装置１０４の署名履歴４１０である。

【００３０】

上記のような公開処理を行うことによって、公開機関側装置１０４は、公開した情報を履歴の中に記録しており、またその記録の間には連鎖関係が構築されている。そのため、定期的に公開機関側装置１０４の署名履歴４１０中の最新の署名記録（たとえば、最新の署名記録のハッシュ値）を新聞等、刊行物（以下、新聞と総称する）に公開して、信頼できるものとし、署名履歴の連鎖検証により公開機関自身が不正を行っていないことを証明することができる。なお、以下では、新聞等刊行物に公開した署名記録を新聞公開署名記録と呼ぶ。

【００３１】

新聞公開署名記録は、後から取り消したり、改ざんしたりすることが非常に困難であるので、信頼性の高い署名記録であるといえる。検証者側装置が連鎖検証する際には、この新聞公開署名記録から、検証対象署名の署名記録までの連鎖を検証する。連鎖が確認できれば、検証対象署名の署名記録は、新聞公開署名記録と同等の信頼性があるといえ、正当性が保証される。

【００３２】

ユーザ側装置における連鎖検証の手順を、図５に示す。

【００３３】

検証者側装置は、署名者の公開鍵によって検証対象署名を検証した後、Ｓ５２７で、署名付き文書中の検証対象署名５０１（図３の３１０に相当）（＝「署名３」）と、それに対応する署名番号（＝「３」）を持つ署名者側装置の署名履歴５０２中の、署名記録５０３の署名値５０６（図３の３０６に相当）（＝「署名３」）とが一致するかどうか検証する。ここで、署名者側装置の署名履歴５０２は、検証前に署名者側装置より入手する。

【００３４】

Ｓ５２８で、検証者側装置は、新聞公開署名記録５２６から、公開機関に預託されている署名者側装置の預託公開署名記録５１３に対応する署名者側装置の署名履歴５０２中の署名記録５０９までの検証を行う。具体的には、まず、署名者側装置の預託公開署名記録５１３について、それとともに公開されている公開ID（＝「３５８」）を取得し、次に公開機関側装置１０４の署名履歴において、その公開ID（＝「３５８」）が記録されている署名記録５１８の項目５１９（図４の４０２に相当）署名番号（＝「８７」）を取得する。

【００３５】
次に、取得した署名番号「８７」以降の署名番号を持つ新聞公開署名記録５２６（＝「署名番号９６」）を新聞から取得する。そして、公開機関側装置１０４の署名履歴において、新聞公開署名記録５２６と同じ署名番号（＝「９６」）を持つ署名記録５２４のハッシュ値と新聞公開署名記録５２６が一致するかどうか検証する。
【００３６】
次に、公開機関側装置１０４の署名履歴において、署名記録５２４中の項目５２５（図４の４０３に相当）前回署名記録のハッシュ値（＝「H(P９５)」）と、その１つ前の署名記録５２３のハッシュ値とが一致するかどうか検証する。ハッシュ関数を用いて署名記録と１つ前の署名記録との整合性を調べるこの処理を、公開機関側装置１０４の署名履歴について、新聞公開署名記録に対応する署名番号（＝「９６」）を持つ署名記録５２４から、預託公開署名記録に対応する署名番号（＝「８７」）を持つ署名記録５１８まで繰り返し行う。そして、公開機関側装置１０４の署名記録５１８中の項目５２２（図４の４０７に相当）公開署名記録のハッシュ値（＝「H(S２０)」）と、預託公開署名記録５１３のハッシュ値とが一致するかどうか検証する。最後に、預託公開署名記録５１３と、それに対応する署名者側装置の署名履歴５０２中の署名記録５０９（＝署名番号「２０」）とが一致するかどうか検証する。
【００３７】
検証者側装置は、S５２８での検証に必要な署名者側装置の預託公開署名記録５１３、公開機関の署名履歴５１７、新聞公開署名記録５２６を、検証前に公開機関側装置は、および新聞より入手する。
【００３８】
S５２９で、検証者側装置は、署名者側装置の署名履歴の署名記録５０９中の項目５１１（図３の３０４に相当）前回署名記録のハッシュ値（＝「H(S１９)」）と、その１つ前の署名記録５０８のハッシュ値とが一致するかどうか検証する。ハッシュ関数を用いて署名記録と１つ前の署名記録との整合性を調べるこの処理を、預託公開署名記録５１３に対応する署名番号（＝「２０」）を持つ署名記録５０９から、検証対象署名５０１に対応する署名番号（＝「３」）を持つ署名記録５０３まで繰り返し行う。
【００３９】
文書検証プログラム２０９の処理によるS５２７、S５２８、S５２９の全ての検証が成功であれば、検証対象署名における連鎖検証は成功である。
【００４０】
上記、連鎖検証に必要なデータは、「検証対象署名５０１（図３の３０４に相当）」、「署名履歴５０２（署名記録５０３、５０７～５０９）」、「預託公開署名記録５１３」、「公開機関側装置１０４の署名履歴５１７（署名記録５１８、５２３、５２４）」、「新聞公開署名記録５２６」である。そこで、検証者側装置は、検証記録保存プログラム２１０の処理により、S５３０において、この５つのデータを検証ログに記録する。作成した検証ログは、検証ログ保管領域２１７に保管する。
【００４１】
検証ログの構成例を図６に示す。検証ログ６０１中、６０３（図３の３１０、図５の５０１に相当）は、検証対象署名であり、６０４～６０７は、連鎖検証に利用した検証対象署名の署名者側装置の署名記録である。また、６０８（図５の５１３に相当）は、預託公開署名記録であり、公開IDとともに記録される。６１０～６１２は公開機関側装置１０４の署名記録である。６１３（図５の５２６に相当）は新聞公開署名記録であり、署名番号とともに記録される。この他に、検証ログ作成日６０２や預託公開署名記録の公開場所６０９、新聞公開署名記録が記載されている新聞社名６１４、検証に利用した公開鍵６１５などの付加情報を記録しても良い。
【００４２】
検証ログ６０１には、検証対象署名６０３（図３の３１０、図５の５０１に相当）について、連鎖検証を含む署名検証に必要なデータが記録されている。したがって、検証者側

装置は、このログ中に記載されたデータを用いて、図５を用いて説明した連鎖検証の手順を再度行うことによって、検証ログに記載された署名６０３（図３の３１０、図５の５０１に相当）の検証と検証ログの正当性の検証を行うことができる。すなわち、検証ログは、署名の正当性証明書であるともいえる。

【００４３】

検証ログに記載された検証対象署名６０３（図３の３１０、図５の５０１に相当）が、署名記録６０４～６０７、預託公開署名記録６０８（図５の５１３に相当）、公開機関側装置１０４の署名記録６１０～６１２、新聞公開署名記録６１３、公開鍵６１５を用いて検証でき、かつ検証ログに記載された新聞公開署名記録６１３（図５の５２６に相当）が新聞に記載されているものと一致すれば、検証ログに記載されている検証対象署名６０３は正当であるといえる。本実施形態の方法によれば、例え署名者側装置の署名履歴が消失してしまっても、検証者側装置は、検証ログから検証に利用したデータを抽出し、公開鍵を用いた署名検証および、S５２７、S５２８、S５２９の検証を行うことによって、検証ログに記載されている署名の正当性を提示することができる。

【００４４】

また、検証ログの方を先に消失してしまった場合でも、検証者側装置は、再度連鎖検証を行い、検証記録保存機能を用いることによって、検証ログを再作成することができる。

【００４５】

検証ログ６０１は、公開されても良いように、署名履歴には、秘密鍵漏洩やプライバシー漏洩に繋がる危険性があるような情報は含んでいないので、検証ログが公開されても、秘密鍵漏洩やプライバシー漏洩することはない。そのため、検証者側装置が、検証ログを公開して、第三者の手によって検証させることも可能である。

【００４６】

また、検証ログが改ざんされた場合、検証対象署名６０３（図３の３１０、図５の５０１に相当）について、検証者側装置は、改ざんされてしまった後の検証ログを用いた検証は行えなくなるが、預託公開署名記録から検証対象署名へと繋がる連鎖の整合性は取れなくなるので、不正な署名の検証が成功となることはない。また、検証ログは、そこに記載されている検証対象署名のみに関する検証結果であるので、検証ログが改ざんされても、そこに記載されている署名以外の他の署名の検証結果に影響を及ぼしたりすることはない。

【００４７】

検証ログは、ユーザ側装置（署名者側装置あるいは検証者側装置、またはその双方）が保管しても良いが、重要文書については、検証ログを、公的な信頼できる第三者機関に預ける、もしくは公的な信頼できる第三者機関側装置に署名してもらうことで、より安全性を高めることができる。検証ログには、秘密鍵漏洩やプライバシー漏洩に繋がる危険性があるような情報は含まれていないので、検証ログを預託することによって秘密鍵漏洩やプライバシー漏洩が生じる危険性はない。

【００４８】

公開機関側装置１０４は、ユーザから署名記録を受け取り、それを公開する第三者機関側装置である。公開した署名記録を預託公開署名記録と呼ぶ。各ユーザにおいて、預託公開署名記録を、署名の連鎖検証の際の起点として利用することによって、預託公開署名記録から連鎖を辿ることができた署名は、公開機関側装置１０４に公開したのと同等の信頼性を得ることができ、署名の長期証拠性を保証することができる。

【００４９】

また、公開機関側装置１０４は、図７に示す以下のようなサービスを提供してもよい。これによって、以下のような効果が得られる。

【００５０】

上記実施例では、預託公開署名記録の公開のタイミングは、ユーザ側装置からの預託公開署名記録の送付に依存しているが、図７に示すサービスによれば、ユーザ側において公開するのを忘れても、連鎖検証が困難になることはない。

【００５１】
また、署名の連鎖検証が可能となるのは、その署名が作成されて以降、署名者側装置が公開機関側装置１０４を利用して預託公開署名記録を作成した時点である。図７に示すサービスによれば、検証対象の署名の署名者側装置と検証者側装置が異なる場合であっても、検証者側装置は連鎖検証可能となったかどうかを知るためには、署名者側装置の署名記録が公開されたかどうかを確認する必要がなくなる。
【００５２】
また、ヒステリシス署名の場合、署名の検証には、署名者側装置の署名履歴、署名者側装置の預託公開署名記録が必要であるが、図７に示すサービスによれば、検証対象の署名の署名者側装置と検証者側装置が異なる場合であっても、検証者がこれらを集める必要がなく、また、署名者が非協力的であっても、検証が可能である。
【００５３】
また、図７に示すサービスに用いる公開機関側装置１０４の構成を図８に示す。
【００５４】
公開機関側装置１０４は、図８に示すように、署名を作成して署名付き文書を送信する送信プログラム８０７と、署名付き文書を受信して署名を検証する受信プログラム８０８と、ユーザから受け取った預託公開署名記録７０５（図５の５１３に相当）をWeb等に公開する公開プログラム８０９と、一定期間公開が無いユーザに対して、公開催促書７０６を送信する公開催促プログラム８１０と、公開通知依頼書７０７を送ってきたユーザに対して、公開通知書７０８を送信する公開通知プログラム８１１と、検証対象署名付き検証依頼書７０９を送ってきたユーザに対して、検証対象署名を検証し、検証結果が書かれた検証ログを送付する検証代行プログラム８１２と、ユーザから署名履歴を受け取る履歴受信プログラム８１３と、各ユーザについての公開情報が記録された公開データベース８１４と、公開通知依頼書を送ってきたユーザについての情報と公開通知処理状況が記録された公開通知依頼データベース８１５と、検証代行について、検証代行依頼書を送ってきたユーザについての情報と検証代行処理状況が記録された検証状況データベース８１６と、ユーザから受け取った署名履歴を保管する署名履歴保管領域８１７と、ユーザから受け取った預託公開署名記録を保管する公開署名記録保管領域８１８と、ユーザから受け取った検証代行依頼書を保管する検証代行依頼書保管領域８１９と、公開機関側装置１０４が作成したあるいはユーザより預託された検証ログを保管する検証ログ保管領域８２０が格納されている記憶装置８０２と、ネットワークを介して他の装置と通信を行うための通信装置８０４と、キーボードやマウスなどの入力装置８０５と、ディスプレイなどの表示装置８０６と、CPU８０１と、これらを接続するインタフェース８０３とから構成される。
【００５５】
以下の説明における各プログラムの処理は、ＣＰＵ８０１が各プログラムを実行することにより、公開機関側装置１０４上で実現されるものである。各プログラムは、予め記憶装置８０２に格納されていてもよいし、公開機関側装置１０４が利用可能な媒体を介して導入されてもよい。媒体とは、たとえば、公開機関側装置１０４に着脱可能な記憶媒体や、通信装置８０４に接続するネットワークまたはネットワークを伝搬する搬送波といった通信媒体を含む。
【００５６】
公開サービス７０１は、公開機関側装置１０４がユーザから預託公開署名記録７０５（図５の５１３に相当）を受け取り、それを自身のデータベースに保管、あるいはWebなどに公開するサービスである。ユーザは、本サービスを利用して、自身の署名履歴中に連鎖検証の際の起点となる信頼性の高い署名記録を生成することができる。
【００５７】
公開処理の流れを図９に示す。
【００５８】
公開機関側装置１０４は、公開サービス７０１を行う際、公開プログラム８０９により、以下のS９０１～S９０６の公開処理を行う。

【００５９】
Ｓ９０１で公開機関側装置１０４はユーザより公開を依頼するデータ（預託公開署名記録）を受け取り、Ｓ９０２でその受け取ったデータを保管、あるいはWebなどに公開する。その際、預託公開署名記録には識別のための固有の公開ID（項目１００３）を付与する。預託公開署名記録は公開IDとともに公開署名記録保管領域８１８に保管される。
【００６０】
Ｓ９０２により、公開機関側装置１０４は、公開したデータ（預託公開署名記録）について、Ｓ９０３で、ユーザ名（項目１００２）、公開ID（項目１００３）、預託公開署名記録の署名番号（項目３０２、項目１００４）、公開日（項目１００６）、公開場所(あるいは保管場所)（項目１００５）を、公開機関側装置１０４の公開データベース８１４に登録する。
【００６１】
公開データベースの構成例を図１０に示す。公開データベースには、ユーザごとに公開ID１００３、公開した預託公開署名記録の署名番号１００４（図3の３０２に相当）、公開場所１００５、公開日１００６が記録され、この公開データベースを参照することによって、どのユーザのどのような情報をいつどこに公開したかを知ることができる。
【００６２】
その後、Ｓ９０４で、公開機関側装置１０４は、公開通知依頼データベース８１５を参照し、今回の公開に関わるユーザについて、他のユーザから公開通知依頼があるかどうか調べ、ある場合は、Ｓ９０５で公開通知処理（Ｓ１２０３、Ｓ１２０４）を行う。公開通知依頼データベース８１５の詳細および、公開通知処理の詳細は、後述の公開通知サービスの説明のところで述べる。
【００６３】
Ｓ９０４で、公開機関側装置１０４は、今回の公開に関わるユーザについて、他のユーザから公開通知依頼が無ければ、Ｓ９０６に進む。
【００６４】
Ｓ９０６では、公開機関側装置１０４は、公開データを受け取り正常に公開した旨を公開依頼ユーザに伝える文書を作成し、公開依頼ユーザに送信する。
【００６５】
公開催促サービス７０２は、一定期間公開が無いユーザに対して、公開機関側装置１０４が公開を催促するサービスである。これにより、ユーザ側における公開忘れを防止し、預託公開署名記録が無いために連鎖検証が困難となるといった状況を防ぐ。
【００６６】
公開催促処理の流れを図１１に示す。
【００６７】
公開機関側装置１０４は、公開催促サービス７０２を行う際、公開催促プログラム８１０により、以下のＳ１１０１～Ｓ１１０４の公開催促処理を行う。
【００６８】
Ｓ１１０１において、公開機関側装置１０４は、Ｓ９０３で預託公開署名記録が登録された公開データベース１００１の各ユーザの最新の公開データに対して、項目「公開日」（１００６）および項目「催促日」（１００７）を参照し、一定期間（例えば、一ヶ月）経過しているものについて、ユーザ名を抽出する。
【００６９】
図１０の例では、現在日時が２００３年９月１０日であるとすると、各ユーザの最新の公開データ（レコード１００９、１０１０、１０１２、１０１５）のうち、レコード１００９、１０１５は前回の公開から一ヶ月以上経過しており、レコード１０１２は、前回の催促日から一ヶ月以上経過しているので、それぞれのレコードの項目「ユーザ名」（１００２）からユーザA、ユーザC、ユーザDが抽出される。
【００７０】
Ｓ１１０２において、公開機関側装置１０４は、Ｓ１１０１で抽出したユーザに送信する

ための公開催促書７０６（公開を催促する文書）を作成し、Ｓ１１０３で、その公開催促書を送信する。ユーザ名と送信先（メールアドレスなど）の対応付けは、上記データベース１００１に新たに項目を追加して送信先を記録することによって行っても良いし、ユーザ名と送信先（メールアドレスなど）を対応付けるためのデータベースを別に作成することによって行っても良い。

【００７１】

最後に、Ｓ１１０４において、公開機関側装置１０４は、公開催促書を送信したことを記録するために、催促したユーザについて、催促対象となった各ユーザの最新のレコードの項目「催促日」（１００７）に公開催促書送信日を記録する。

【００７２】

公開通知サービス７０３は、公開通知依頼７０７に従って、あるユーザに関わる公開が行われたことを、公開機関側装置１０４が公開通知７０８によって、別のユーザに通知するサービスである。検証者側装置は、署名者側装置の預託公開署名記録が公開されたことを公開機関側装置１０４より通知してもらうことによって、検証対象署名が署名者側装置の署名履歴を用いて連鎖検証することが可能となったことを知ることができる。

【００７３】

公開通知処理の流れを図１２に示す。

【００７４】

公開機関側装置１０４は、公開通知サービス７０３を行う際、公開通知プログラム８１１の実行により、以下のＳ１２０１～Ｓ１２０４の公開通知処理を行う。

【００７５】

Ｓ１２０１で、公開機関側装置１０４は、ユーザAより「ユーザBに関わる預託公開署名記録が次に公開された時、連絡下さい」との公開通知依頼書を受け取ると、公開機関側装置１０４はＳ１２０２で、その公開通知依頼内容を公開通知依頼データベース８１５に登録する。

【００７６】

公開通知依頼データベース１３０１（図８の８１５）の構成を図１３に示す。公開通知依頼データベース１３０１には、公開通知の対象となる公開者「被依頼ユーザ名」（１３０２）、公開通知依頼者情報「公開依頼ユーザ名(メールアドレス)」（１３０３）、公開通知依頼日を表す「依頼日」（１３０４）、公開通知済であるか否かを表す「通知有無」（１３０５）を登録する。上記例では、被依頼ユーザ名は「ユーザB」、公開通知依頼ユーザ名は「ユーザA」となる。

【００７７】

図９の公開処理において、Ｓ９０４で、公開機関側装置１０４は、公開通知依頼データベース１３０１を参照し、今回公開した公開署名記録に対して、他のユーザから公開通知依頼があるかどうか調べ、ある場合は、以下の通知書送信処理を行う。

【００７８】

まず、Ｓ１２０３で、公開機関側装置１０４は、今回の公開（預託公開署名記録の公開を依頼したユーザ側装置に関わる公開）について通知を依頼したユーザを抽出する。例えば、今回の公開者がユーザBである場合、公開通知依頼データベースの項目「被依頼ユーザ名」（１３０２）がユーザBであるレコード１３０６の項目「依頼ユーザ名」（１３０３）より、ユーザAが抽出される。

【００７９】

Ｓ１２０４で、公開機関側装置１０４は、Ｓ１２０３で抽出したレコードの項目「通知有無」（１３０５）が「未」であれば、Ｓ１２０３で抽出したユーザに対して公開通知書７０８を送信する。送信後、Ｓ１２０３で抽出したレコードの項目「通知有無」（１３０５）に送信日を記録する。

【００８０】

検証代行サービス７０４は、ユーザ（検証者）側装置に代わって、公開機関側装置１０４が署名の検証を行うサービスである。検証に必要な署名者側装置の署名履歴や預託公開

署名記録の収集といった検証者の手間を減らすことができる。また、公的な第三者機関側装置である公開機関側装置１０４が、検証結果を前述の検証ログとして公開することで、署名の有効性をより高い信頼性で保証するとともに、長期に渡って検証結果を保証することができる。公開された検証ログには、検証に利用したデータが記載されているので、公開機関側装置１０４に限らず誰でもその内容を再検証することが可能である。

【００８１】

検証代行サービス７０４は、検証代行依頼書受信処理と署名検証処理の2つに分けられる。検証代行依頼書受信処理の流れを図１４に、署名検証処理の流れを図１５に示す。

【００８２】

公開機関側装置１０４は、検証代行サービス７０４を行う際、検証代行プログラム８１２により、以下のS１４０１～S１４０６の検証代行依頼書受信処理、およびS１５０１～S１５０８の署名検証処理を行う。

【００８３】

S１４０１で公開機関側装置１０４は、検証者側装置より検証代行依頼書７０９を受け取る。検証代行依頼書には、検証対象署名付き文書、署名者名（メールアドレス）、検証代行依頼者名（メールアドレス）が記載されている。

【００８４】

S１４０２で、公開機関側装置１０４は、S１４０１で受け取った検証代行依頼書に対し、固有の検証IDを付与する。検証IDが付けられた検証代行依頼書は、検証代行依頼書保管領域８１９に保管する。

【００８５】

S１４０３において、公開機関側装置１０４は、検証対象署名の署名番号（項目３０２）以降で、検証対象署名の署名者側装置により公開を預託された公開データ（預託公開署名記録（図５の５１３に相当））があるかどうか、公開データベース１００１の項目「ユーザ名」（１００２）および項目「署名番号」（１００４（図３の３０２に相当））により調べる。具体的には、検証対象署名の署名者と同じユーザ名を持つレコードを抽出し、抽出したレコードに対して、項目「署名番号」（１００４（図３の３０２に相当））を調べ、検証対象署名の署名番号より大きくかつ直近の署名番号を持つレコードを抽出する。目的の公開データが無い場合は、S１４０６に進む。

【００８６】

S１４０４において、公開機関側装置１０４は、検証対象署名が検証できるような署名履歴が署名履歴保管領域８１７に存在するかどうか調べる。具体的には、検証対象署名の署名者側装置の署名履歴であり、かつ検証対象署名の署名番号からS１４０３で抽出したレコードの署名番号までの範囲を含んでいる署名履歴が、署名履歴保管領域に存在しているか調べる。既に存在していれば、S１４０６に進み、存在していなければ、S１４０５において、検証対象署名の署名者側装置に対し、検証対象署名の署名番号からS１４０３で抽出したレコードの署名番号までの範囲を含んでいる署名履歴の送付を要請する。

【００８７】

S１４０６で、公開機関側装置１０４は、現段階の検証状況を検証状況データベースに記録する。

【００８８】

検証状況データベース１６０１（図８の８１６）の構成を図１６に示す。検証状況データベース１６０１には、S１４０２で生成した「検証ID」（１６０２）、検証代行依頼者を表す「依頼ユーザ名」（１６０３）、検証対象署名の署名者を表す「検証対象署名者」（１６０４）、検証に利用する公開書名記録の公開IDを示す「公開ID」（１６０５）、検証依頼日を示す「依頼日」（１６０６）、検証状況を示す「検証状況」（１６０７）が記録される。検証ID１６０２は、検証代行依頼書と検証状況データベースのレコードとを対応付ける。また、検証状況１６０７には、S１４０３で預託公開署名記録が存在していなかったことを示す「公開記録無」、S１４０４で署名履歴が存在していたことを示す「履歴取得済」、S１４０４で署名履歴が存在しておらず、署名履歴を検証対象署名の署名者

側装置に要請中であることを示す「履歴取得中」、既に検証が終了していることを示す「検証完了」といった情報が記録される。

【００８９】

検証代行依頼書受信処理が終了した検証代行依頼については、次の署名検証処理を行う。

【００９０】

署名検証処理を行うタイミングとしては、検証代行依頼書受信処理が終了した直後、あるいは、１日おきなど一定間隔、あるいは、Ｓ１４０５で要請した署名履歴が、ユーザより送付され、履歴受信プログラム８１３により、受け取った署名履歴が署名履歴保管領域８１７に保存された時などがある。

【００９１】

公開機関側装置１０４の履歴受信プログラム８１３は、受け取った署名履歴および送信者名を署名履歴保管領域８１７に保存するとともに、検証状況データベース１６０１の該当するレコードの項目「検証状況」（１６０７）に「履歴取得済」を記録する。該当するレコードとは、検証状況データベース１６０１の項目「検証対象署名者」（１６０４）と署名履歴送信者が同じであり、かつ項目「検証ID」（１６０２）に対応する検証代行依頼書（検証代行依頼書保管領域に保管されている）の検証対象署名の署名番号から項目「公開ID」（１６０５）に対応する預託公開署名記録（公開署名記録保管領域に保管されている）の署名番号までの範囲が履歴受信プログラムで受信した署名履歴に含まれているレコードである。

【００９２】

署名検証処理においては、まず、Ｓ１５０１で、公開機関側装置１０４は、検証状況データベース１６０１において、今から検証を行う検証代行依頼書について、検証ID１６０２を参照して該当するレコード（検証IDが検証代行依頼書の検証IDと一致するレコード。検証対象レコードと呼ぶ）を抽出し、検証状況１６０７を確認する。検証代行依頼書に添付されている署名（ユーザが検証を依頼した署名）を以降、検証対象署名と呼ぶ。

【００９３】

Ｓ１５０１において、検証状況１６０７が、「公開記録無」の場合は、Ｓ１５０６へと進み、公開機関側装置１０４は、検証代行依頼書の検証対象署名の署名番号（項目４０２）以降で、検証対象署名の署名者側装置により公開を預託された預託公開署名記録があるかどうか、公開データベース１００１の項目「ユーザ名」（１００２）および項目「署名番号」（１００４）により調べる。具体的には、検証対象署名の署名者と同じユーザ名を持つレコードを抽出し、抽出したレコードに対して、項目「署名番号」（１００４）を調べ、検証対象署名の署名番号より大きくかつ直近の署名番号を持つレコードを抽出する。目的の預託公開署名記録が無い場合は、署名検証処理を終了する。

【００９４】

Ｓ１５０６で、検証対象署名の署名者側装置の該当する預託公開署名記録があった場合、公開機関側装置１０４は、Ｓ１５０７において、検証対象署名が検証できるような署名履歴が署名履歴保管領域８１７に存在するかどうか調べる。具体的には、検証対象署名の署名者側装置の署名履歴であり、かつ検証対象署名の署名番号からＳ１５０６で抽出したレコードの署名番号までの範囲を含んでいる署名履歴が、署名履歴保管領域に存在しているか調べる。

【００９５】

既に存在していれば、Ｓ１５０２に進む。存在していなければ、Ｓ１５０８において、検証対象署名の署名者側装置に対し、検証対象署名の署名番号からＳ１５０６で抽出したレコードの署名番号までの範囲を含んでいる署名履歴の送付を要請し、Ｓ１５０４に進む。Ｓ１５０４では、公開機関側装置１０４は、検証状況データベース１６０１において、検証対象の検証代行依頼書について、検証ID１６０２を参照して検証IDが検証代行依頼書の検証IDと一致するレコードを抽出し、検証状況１６０７に「履歴取得中」を記録して、署名検証処理を終了する。

【００９６】
Ｓ１５０１において、検証状況１６０７が、「履歴取得中」の場合は、Ｓ１５０５へと進み、公開機関側装置１０４は、検証対象署名が検証できるような署名履歴が署名履歴保管領域８１７に存在するかどうか調べる。具体的には、検証対象署名の署名者側装置の署名履歴であり、かつ検証対象署名の署名番号から検証対象署名の署名者側装置の預託公開署名記録の署名番号までの範囲を含んでいる署名履歴が、署名履歴保管領域に存在しているか調べる。
【００９７】
ここで、検証対象署名の署名者側装置の預託公開署名記録の署名番号は、次のようにして求める。まず、検証対象の検証代行依頼書の検証IDを取得し、検証状況データベース１６０１において、検証ID１６０２を参照して該当するレコード（検証IDが検証代行依頼書の検証IDと一致するレコード）を抽出する。抽出したレコードにおいて、公開ID１６０５を取得する。
【００９８】
次に、公開データベース１００１において、公開ID１００３を参照して該当するレコード（公開IDが検証状況データベースより抽出したレコードの公開ID１６０５と一致するレコード）を抽出し、そのレコードの署名番号１００４を取得する。この署名番号が、検証対象署名の署名者側装置の預託公開署名記録の署名番号である。検証対象署名が検証できるような署名履歴が署名履歴保管領域８１７に存在していれば、Ｓ１５０２に進み、存在していなければ、署名検証処理を終了する。
【００９９】
Ｓ１５０１において、検証状況１６０７が「履歴取得済」である場合は、Ｓ１５０２へと進む。
【０１００】
Ｓ１５０１において、検証状況１６０７が「検証完了」である場合は、署名検証処理を終了する。
【０１０１】
Ｓ１５０２では、公開機関側装置１０４は、検証代行依頼書より検証対象署名５０１（図３の３１０に相当）を取得し、Ｓ１５０１で抽出した検証対象レコードの項目「検証対象署名者」（１６０４）の署名履歴であり、かつ検証対象署名の署名番号から検証対象署名の署名者側装置の預託公開署名記録の署名番号までの範囲を含んでいる署名履歴を取得する。
【０１０２】
ここで、検証対象署名の署名者側装置の預託公開署名記録の署名番号は、次のようにして求める。まず、検証対象の検証代行依頼書の検証IDを取得し、検証状況データベース１６０１において、検証ID１６０２を参照して該当するレコード（検証IDが検証代行依頼書の検証IDと一致するレコード）を抽出する。抽出したレコードにおいて、公開ID１６０５を取得する。
【０１０３】
次に、公開データベース１００１において、公開ID１００３を参照して該当するレコード（公開IDが検証状況データベースより抽出したレコードの公開ID１６０５と一致するレコード）を抽出し、そのレコードの署名番号１００４を取得する。この署名番号が、検証対象署名の署名者側装置の預託公開署名記録の署名番号である。
【０１０４】
また、検証対象レコード中の公開ID１６０５に対応する預託公開署名記録５１３を公開署名記録保管領域より取得する。そして、以上取得したデータの検証対象署名５０１（図３の３１０に相当）、検証対象署名の署名者側装置の署名履歴５０２、検証対象署名の署名者側装置の預託公開署名記録５１３、公開機関側装置１０４の署名履歴５１７、新聞公開署名記録５２６を用いて、図５のＳ５２７、Ｓ５２８、Ｓ５２９の処理を行い、検証対象署名を検証する。

【０１０５】
Ｓ１５０３において、Ｓ１５０２での検証に利用したデータ「検証対象署名５０１（図３の３１０に相当）」「署名履歴５０２（署名記録５０３、５０７～５０９）」「預託公開署名記録５１３」「公開機関側装置１０４の署名履歴５１７」「新聞公開署名記録５２６」を記録した検証ログを作成し、検証対象レコードの項目「依頼ユーザ名（メールアドレス）」（１６０３）を参照して検証代行依頼ユーザに、作成した検証ログ７１０（図６の６０１に相当）を送信する。

【０１０６】
最後に、Ｓ１５０４において、検証対象レコードの項目「検証状況」（１６０７）に「検証完了」を記録する。

【０１０７】
また、署名検証処理終了後、検証状況データベース中の項目「依頼日」（１６０６）を参照して、一定期間が経過しているにもかかわらず検証状況が「検証完了」になっていないレコードを抽出し、そのレコードに該当する検証代行依頼書については、検証できなかった旨を伝える文書を検証代行依頼者１６０３に送信する。

【０１０８】
ここで、以下のような状況における本実施形態における検証代行の流れを図１７を用いて述べる。

【０１０９】
今、ユーザB側装置は、ユーザA側装置よりAのヒステリシス署名付き契約書（有効期間５年間）１７０１を３ヶ月前に受信したとする。ヒステリシス署名は、長期証拠性を維持する署名技術であるが、ユーザA側装置の作成した署名を検証するためには、ユーザA側装置がきちんと署名履歴を保管しておく必要があり、契約書の証拠性は、ユーザA側装置の署名履歴保持に依存している。このような場合、契約書の証拠性を高めるためにユーザB側装置は、公開機関側装置１０４に検証代行を依頼し、検証ログを発行してもらうことができる。

【０１１０】
まず、ユーザB側装置は、ユーザA側装置のヒステリシス署名付き契約書（以降、検証対象署名と呼ぶ。署名番号は「１０」）を添付した検証代行依頼書１７０２（図７の７０９に相当）を作成し、公開機関側装置１０４に送信する。

【０１１１】
ユーザB側装置より検証代行依頼書１７０２（図７の７０９に相当）を受け取った公開機関側装置１０４は、検証代行プログラム８１２の処理により、図１４、図１５の検証代行処理を行う。Ｓ１４０１で受け取った検証代行依頼書１７０２（図７の７０９に相当）に対して、Ｓ１４０２で検証IDを作成する。本例では、検証ID「０００００１」が作成された。検証代行依頼書１７０２（図７の７０９に相当）は、検証ID「０００００１」とともに、公開機関側装置１０４の検証代行依頼書保管領域８１９に保管される。

【０１１２】
公開機関側装置１０４では、Ｓ１４０３において、検証対象署名の署名番号（「１０」）以降で、検証対象署名の署名者ユーザA側装置により公開を預託された預託公開署名記録があるかどうか、公開データベース１００１の項目「ユーザ名」（１００２）および項目「署名番号」（１００４）により調べる。その結果、レコード１００９は、項目「ユーザ名」が「ユーザA」であり、項目「署名番号」が「３２」で検証対象署名の署名番号「１０」より大きいので、該当するレコードである。

【０１１３】
Ｓ１４０４において、公開機関側装置１０４は、検証対象署名の署名者「ユーザA」の署名履歴であり、かつ検証対象署名の署名番号「１０」からＳ１４０３で抽出したレコードの署名番号「３２」までの範囲を含んでいる署名履歴が、公開機関側装置１０４の署名履歴保管領域８１７に存在しているか調べる。本例では、存在していなかったので、Ｓ１４０５において、公開機関側装置１０４は、検証対象署名の署名者「ユーザA」に対し、検

証対象署名の署名番号「１０」からS１４０３で抽出したレコードの署名番号「３２」までの範囲を含んでいる署名履歴の送付を要請する。

【０１１４】

S１４０６で、公開機関側装置１０４は、現段階の検証状況を検証状況データベース１６０１に記録して、検証代行依頼書受信処理を終了する。本例について記録したものがレコード１６０８である。「検証ID」（＝０００００１）、「依頼ユーザ名」（＝ユーザB）、「検証対象署名者」（＝ユーザA）、「公開ID」（＝０００１４２）、「依頼日」（＝２００３年９月１０日）、「検証状況」（＝履歴取得中）である。

【０１１５】

署名履歴の送付を要請していたユーザA側装置より署名履歴が送られてきたら、公開機関側装置１０４は、履歴受信プログラム８１３により、受け取ったユーザA側装置の署名履歴および送信者名「ユーザA」を署名履歴保管領域８１７に保存するとともに、検証状況データベース１６０１の項目「検証対象署名者」（１６０４）について署名履歴送信者「ユーザA」と同じであるレコード１６０８を抽出する。

【０１１６】

次に、レコード１６０８の項目「検証ID」（＝０００００１）に対応する検証代行依頼書１７０２（図７の７０９に相当）（検証代行依頼書保管領域に保管されている）を調べ、添付されている検証対象署名の署名番号「１０」からレコード１６０８の項目「公開ID」（＝０００１４２）に対応する預託公開署名記録（公開署名記録保管領域に保管されている）の署名番号「３２」までの範囲が履歴受信プログラムで受信した署名履歴に含まれていれば、検証状況データベース１６０１のレコード１６０８の項目「検証状況」に「履歴取得済」を記録する。

【０１１７】

検証に必要な署名履歴が取得されたタイミングで、公開機関側装置１０４は、上記レコード１６０８の検証依頼（検証ID「０００００１」の検証代行依頼書１７０２（図７の７０９に相当））について、以下の署名検証処理を行う。本例では、このタイミングとしたが、定期的に全レコードに対して署名検証処理を行っても良い。

【０１１８】

署名検証処理においては、まず、S１５０１で、公開機関側装置１０４は、検証状況データベース１６０１において、今から検証を行う検証代行依頼書１７０２（図７の７０９に相当）と同じ検証ID「０００００１」を持つレコード１６０８を抽出し、検証状況を確認する。検証状況１６０７が「履歴取得済」であるので、S１５０２へと進む。

【０１１９】

S１５０２では、公開機関側装置１０４は、検証代行依頼書１７０２（図７の７０９に相当）より検証対象署名付き文書１７０１を取得し、S１５０１で抽出したレコード１６０８の項目「検証対象署名者」（＝「ユーザA」）の署名履歴であり、かつ「検証対象署名の署名番号」（＝「１０」）からレコード１６０８の公開ID（＝「０００１４２」）に対応する「預託公開署名記録の署名番号」（＝「３２」）までの範囲を含んでいる署名履歴を公開機関側装置１０４の署名履歴保管領域８１７より取得する。

【０１２０】

また、レコード１６０８の公開ID（＝「０００１４２」）に対応する預託公開署名記録を公開署名記録保管領域８１８より取得する。そして、検証対象署名と上記取得した署名履歴、預託公開署名記録、公開機関側装置１０４の署名履歴、新聞公開署名記録を用いて、図５のS５２７、S５２８、S５２９の処理を行い、検証対象署名を検証する。

【０１２１】

S１５０３において、公開機関側装置１０４は、S１５０２での検証に利用したデータ「検証対象署名」「署名者側装置の署名履歴」「預託公開署名記録」「公開機関側装置１０４の署名履歴」「新聞公開署名記録」を記録した検証ログ（６０１）を作成し、レコード１６０８の項目「依頼ユーザ名（メールアドレス）」（＝「ユーザB」）を参照して検証代行依頼ユーザ「ユーザB」側装置に作成した検証ログ１７０３（図６の６０１、図７の

７１０に相当）を送信する。

【０１２２】

最後に、公開機関側装置１０４は、Ｓ１５０４において、レコード１６０８の項目「検証状況」に「検証完了」を記録する。

【０１２３】

以上の公開機関側装置１０４の検証代行サービスにより、ユーザAの契約書に対する検証ログ１７０３（図６の６０１、図７の７１０に相当）を受け取ったユーザB側装置は、検証ログに記載されている検証対象署名がユーザA側装置から受け取った契約書の署名と一致していること、また、公開機関側装置１０４のHPなどを参照し、検証ログに記載されている預託公開署名記録が公開機関側装置１０４によって公開されているものと一致していること、あるいは検証ログに記載されている新聞公開署名記録が新聞に掲載されている新聞公開署名記録と一致していることを確認する。

【０１２４】

そして、それらが確認できた検証ログをユーザB側装置の検証ログ保管領域２１７に保管しておく、または公開機関側装置１０４の検証ログ保管領域８２０に保管しておくことによって、ユーザB側装置は、ユーザA側装置に頼らず、いつでも自身の保管する検証ログによって署名の正当性を示すことができる。

【図面の簡単な説明】

【０１２５】

【図１】第１実施形態が適用されたシステムの概略図である。

【図２】第１実施形態におけるユーザ側装置の構成図である。

【図３】ヒステリシス署名技術の概略図である。

【図４】公開機関側装置の公開の仕組みを表した図である。

【図５】検証ログ作成を含む連鎖検証手順を説明するためのフロー図および概念図である。

【図６】検証ログの内容を表した図である。

【図７】本実施形態における公開機関側装置のサービス形態を表した図である。

【図８】本実施形態における公開機関側装置の構成図である。

【図９】公開機関側装置の公開処理のフロー図である。

【図１０】公開機関側装置の公開データベースを表した図である。

【図１１】公開機関側装置の公開催促処理のフロー図である。

【図１２】公開機関側装置の公開通知処理のフロー図である。

【図１３】公開機関側装置の公開通知依頼データベースを表した図である。

【図１４】公開機関側装置の検証代行処理のうち、検証代行依頼書受信処理のフロー図である。

【図１５】公開機関側装置の検証代行処理のうち、署名検証処理のフロー図である。

【図１６】公開機関側装置の検証状況データベースを表した図である。

【図１７】検証代行の例を表した図である。

【符号の説明】

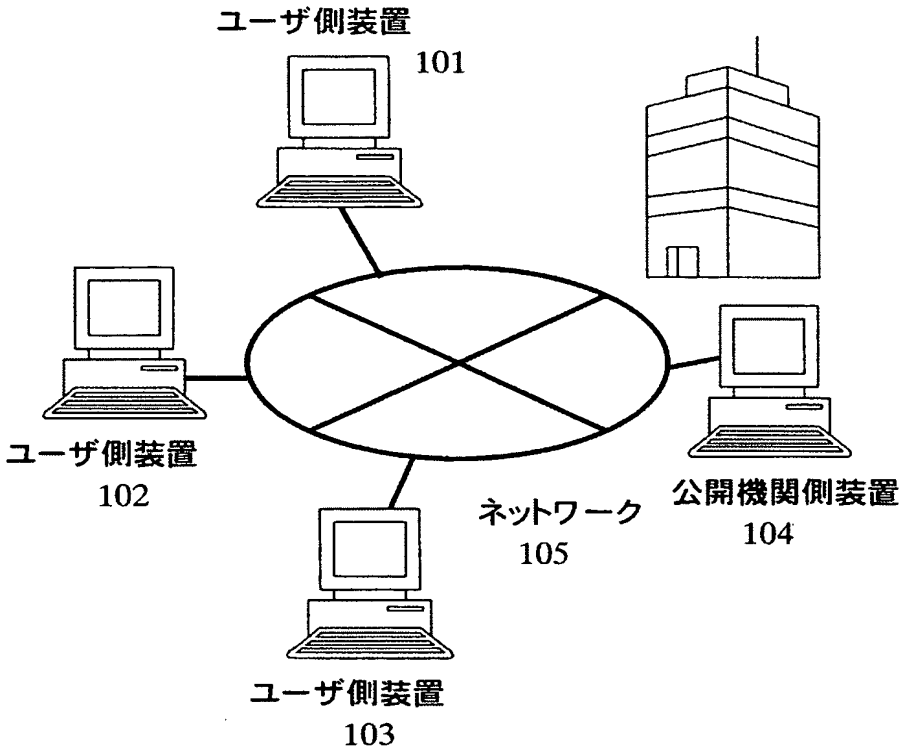
【０１２６】

１０１～１０３：ユーザ側装置、１０４：公開機関側装置、１０５：ネットワーク、３０１：項目（「識別番号」）、３０２：項目（「署名番号」）、３０３：項目（「種別」）、３０４：項目（「前回署名記録のハッシュ値」）、３０５：項目（「文書のハッシュ値」）、３０６：項目（「署名 or 受信署名記録情報」）、３０７：送信文書、３０８、３１０：署名、３０９：受信文書、３１１：署名履歴、３１２～３１５：署名記録、４０１：項目（「識別番号」）、４０２：項目（「署名番号」）、４０３：項目（「前回署名記録のハッシュ値」）、４０４：項目（「署名値」）、４０５：項目（「公開ID」）、４０６：項目（「預託公開署名記録番号」）、４０７：項目（「預託公開署名記録のハッシュ値」）、４０８：公開依頼書、４０９：署名、４１０：公開機関側装置の署名履歴、４１１～４１３：署名記録、５０１：検証対象署名付き文書、５０２：署名履歴、５０３～

５０９：署名記録、５０４、５１０：項目（「署名番号」）、５０５、５１１：項目（「前回署名記録のハッシュ値」）、５０６、５１２：項目（「署名値」）、５１３：預託公開署名記録、５１４：預託公開署名記録の項目（「署名番号」）、５１５：預託公開署名記録の項目（「前回署名記録のハッシュ値」）、５１６：預託公開署名記録の項目（「署名値」）、５１７：公開機関側装置の署名履歴、５１８、５２３、５２４：公開機関側装置の署名記録、５１９：項目（「署名番号」）、５２０、５２５：項目（「前回署名記録のハッシュ値」）、５２１：項目（「公開ID」）、５２２：項目（「預託公開署名記録のハッシュ値」）、５２６：新聞公開署名記録、６０１：検証ログ、６０２：項目（「作成日」）、６０３：項目（「検証署名」）、６０４～６０７：項目（「署名履歴」）、６０８：項目（「預託公開署名記録」）、６０９：項目（「公開場所」）、６１０～６１２：項目（「公開機関側装置の署名履歴」）、６１３：項目（「新聞公開署名記録」）、６１４：項目（「新聞公開先」）、６１５：項目（「公開鍵」）、７０１：公開サービス、７０２：公開催促サービス、７０３：公開通知サービス、７０４：検証代行サービス、７０５：公開を依頼する署名記録、７０６：公開催促書、７０７：公開通知依頼書、７０８：公開通知書、７０９：検証代行依頼書、７１０：検証ログ、１００１：公開データベース、１００２：項目（「ユーザ名」）、１００３：項目（「公開ID」）、１００４：項目（「署名番号」）、１００５：項目（「公開場所」）、１００６：項目（「公開日」）、１００７：項目（「催促日」）、１００８～１０１５：公開データベースのレコード、１３０１：公開通知依頼データベース、１３０２：項目（「被依頼ユーザ名」）、１３０３：項目（「依頼ユーザ名」）、１３０４：項目（「依頼日」）、１３０５：項目（「通知有無」）、１３０６～１３０８：公開通知依頼データベースのレコード、１６０１：検証状況データベース、１６０２：項目（「検証ID」）、１６０３：項目（「依頼ユーザ名」）、１６０４：項目（「検証対象署名者」）、１６０５：項目（「公開ID」）、１６０６：項目（「依頼日」）、１６０７：項目（「検証状況」）、１６０８～１６１１：検証状況データベースのレコード、１７０１：検証対象署名付き文書、１７０２：検証代行依頼書、１７０３：検証ログ

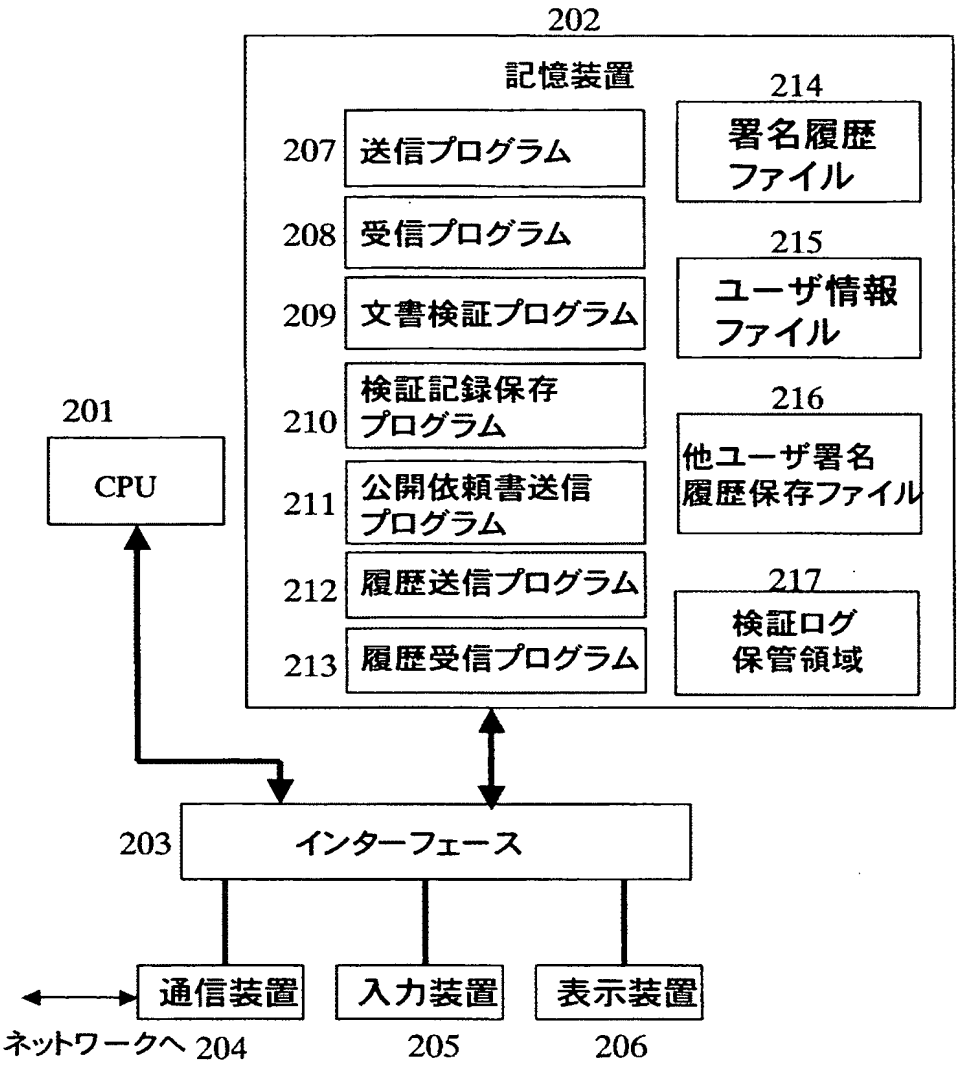
【書類名】図面
【図１】

【図1】

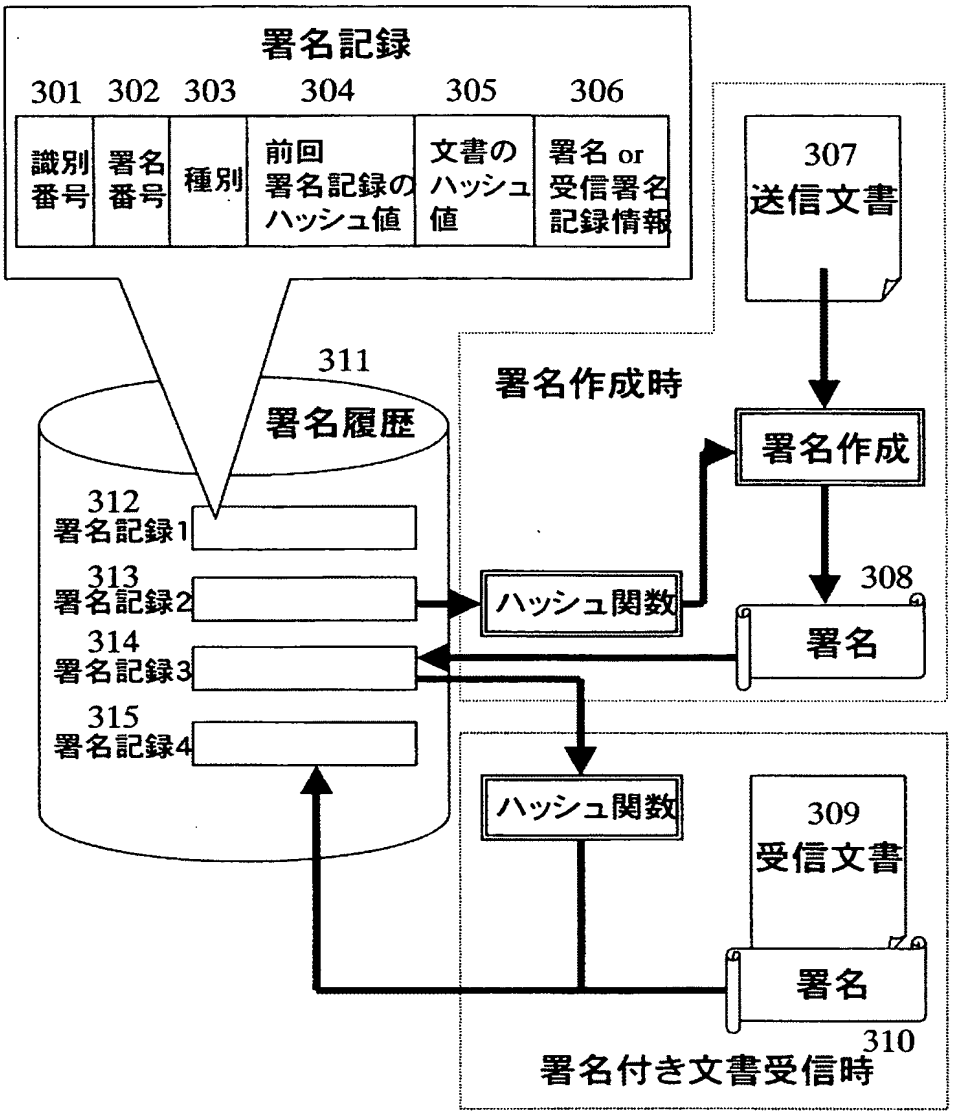


【図２】

【図2】

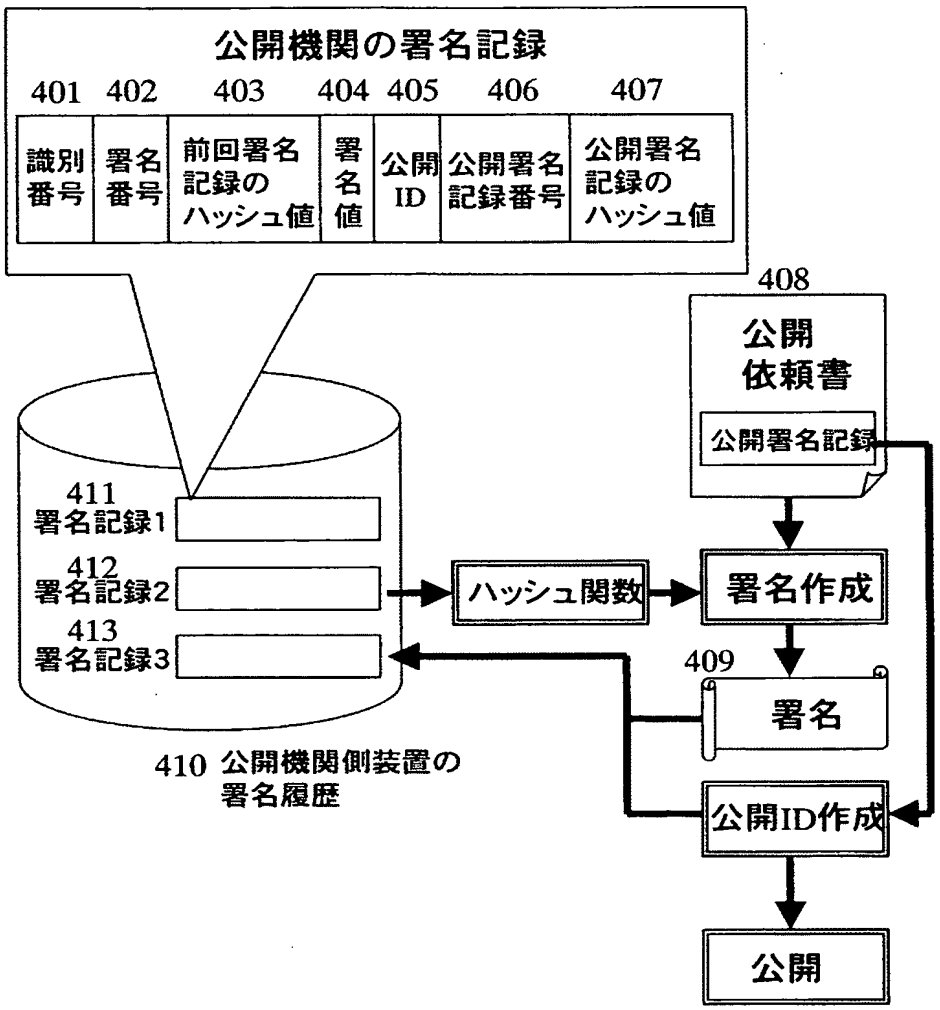

202
記憶装置
207 送信プログラム
208 受信プログラム
209 文書検証プログラム
210 検証記録保存プログラム
211 公開依頼書送信プログラム
212 履歴送信プログラム
213 履歴受信プログラム
214 署名履歴ファイル
215 ユーザ情報ファイル
216 他ユーザ署名履歴保存ファイル
217 検証ログ保管領域
201 CPU
203 インターフェース
通信装置
入力装置
表示装置
ネットワークへ 204
205
206

【図３】

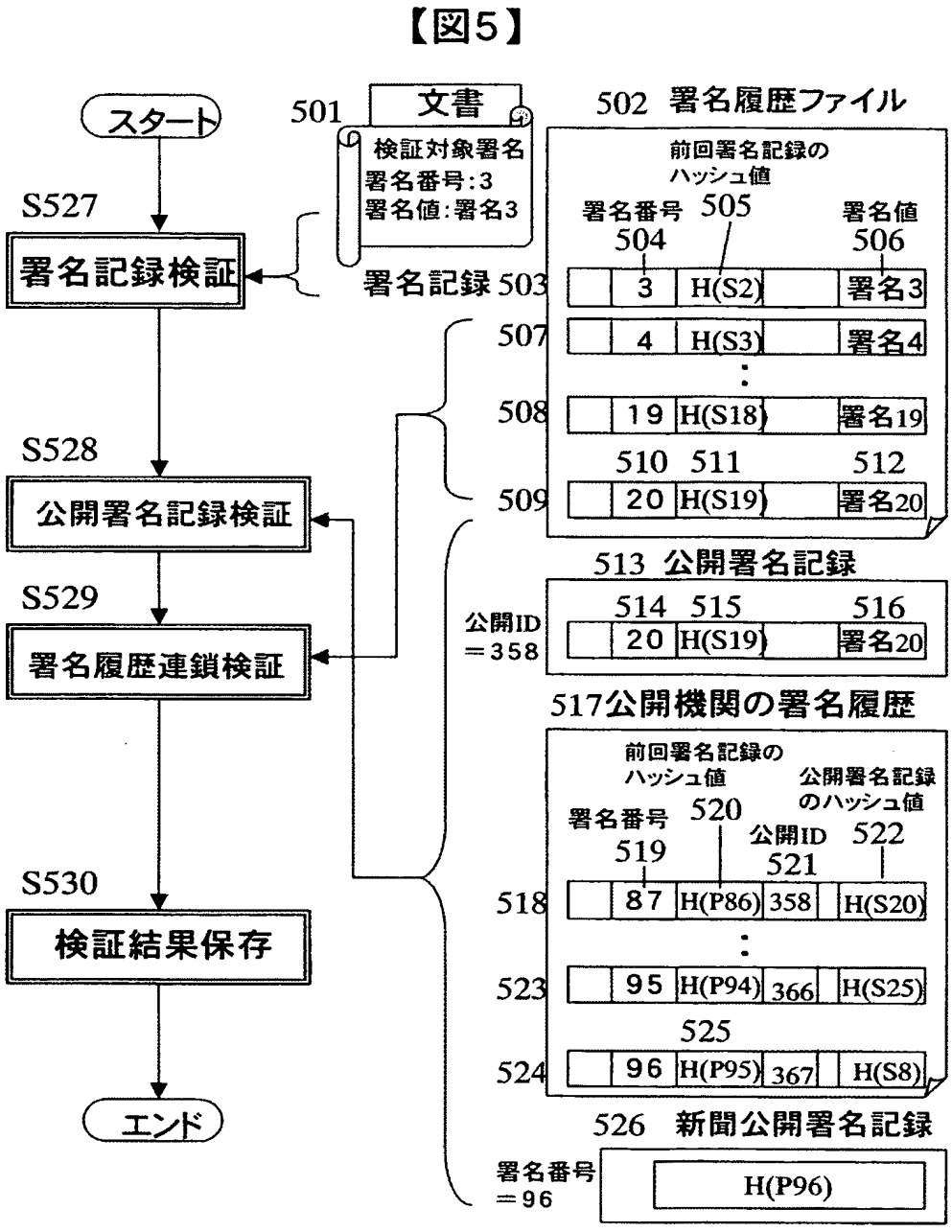

【図3】
署名記録
301
302
303
304
305
306
識別番号
署名番号
種別
前回署名記録のハッシュ値
文書のハッシュ値
署名 or 受信署名記録情報
307
送信文書
311
署名履歴
署名作成時
署名作成
312
署名記録1
313
署名記録2
314
署名記録3
315
署名記録4
ハッシュ関数
308
署名
ハッシュ関数
309
受信文書
署名
310
署名付き文書受信時

【図４】

【図4】


公開機関の署名記録
401
402
403
404
405
406
407
識別番号
署名番号
前回署名記録のハッシュ値
署名値
公開ID
公開署名記録番号
公開署名記録のハッシュ値
408
公開依頼書
公開署名記録
411
署名記録1
412
署名記録2
413
署名記録3
ハッシュ関数
署名作成
409
署名
公開ID作成
公開
410 公開機関側装置の署名履歴

【図５】


【図5】
スタート
S527
署名記録検証
S528
公開署名記録検証
S529
署名履歴連鎖検証
S530
検証結果保存
エンド
501
文書
検証対象署名
署名番号:3
署名値:署名3
署名記録 503
502 署名履歴ファイル
前回署名記録の
ハッシュ値
署名番号 505
504
署名値
506
3 H(S2) 署名3
4 H(S3) 署名4
19 H(S18) 署名19
20 H(S19) 署名20
507
508
509
510 511 512
513 公開署名記録
公開ID
＝358
514 515 516
20 H(S19) 署名20
517公開機関の署名履歴
前回署名記録の
ハッシュ値
公開署名記録
のハッシュ値
署名番号 520
519
公開ID 522
521
87 H(P86) 358 H(S20)
95 H(P94) 366 H(S25)
96 H(P95) 367 H(S8)
518
523
525
524
526 新聞公開署名記録
署名番号
＝96
H(P96)

【図６】

【図6】

601 検証ログ

602 作成日：2003年8月29日

検証署名：

603 01063A78BA216574EC5F77F3315

署名履歴：

604 01063A78BA21657499002DEC5F77F3315

605 01074D830A03B187E3FF22289BAC09121

606 01089BBA21865740BE7F21FE339647381

607 0109E324876529C1D36FA119503645B193

公開署名記録：　公開ID＝３７７

608 0109E324876529C1D36FA119503645B193

609 公開場所（http://www.XXX.co.jp/）

公開機関の署名履歴：

610 011084FA219585944994637290OBC21543

611 01114563B281AEE7E3FF2229DC2190031

612 01124A849035462CD18593404093672874

新聞公開署名記録：署名番号＝１１２

613 01124A849035462CD18593404093672874

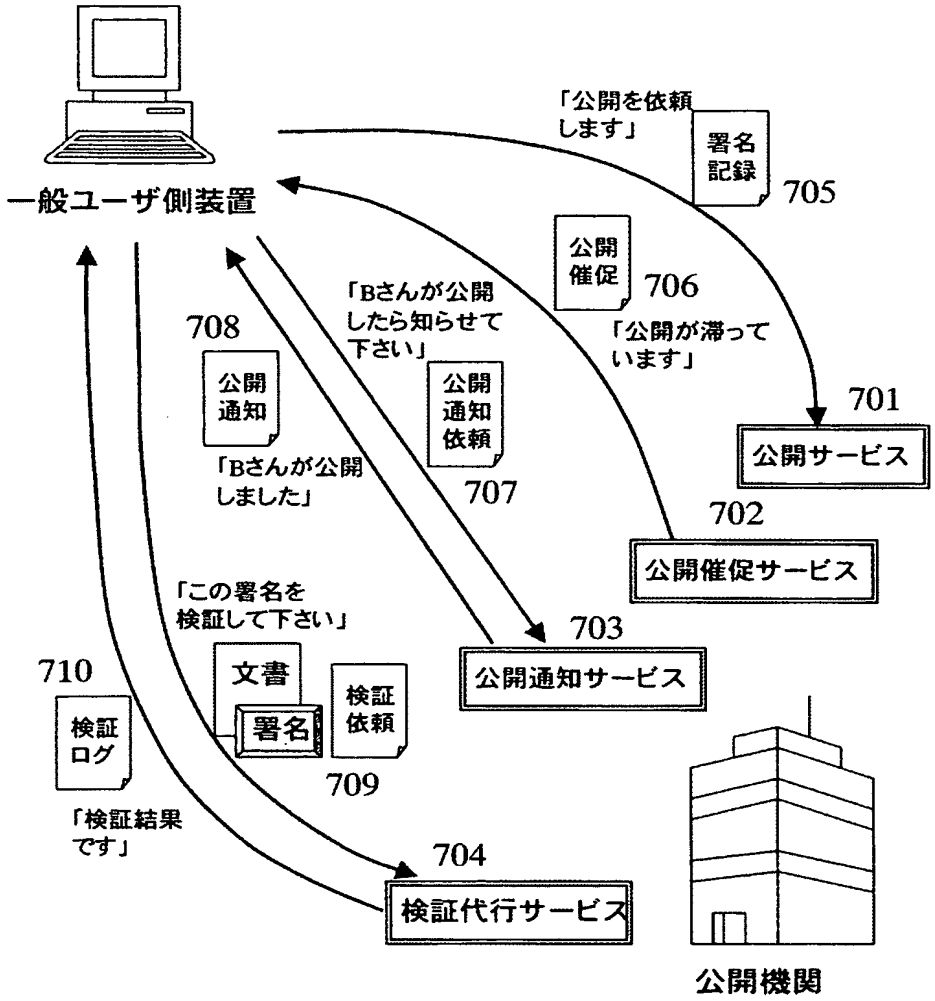
614　○○新聞社2003年9月10日朝刊

公開鍵：

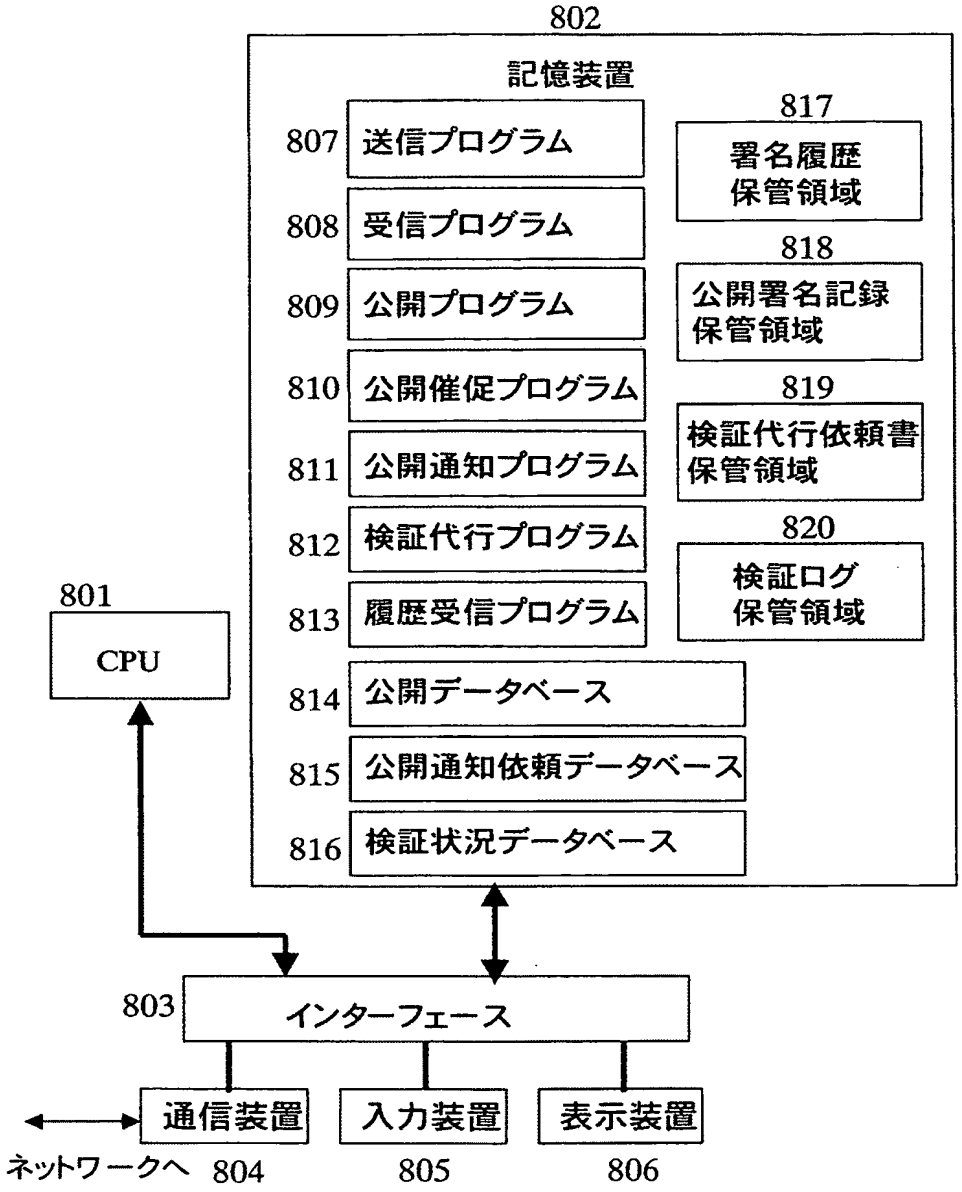
615 C7A437BA9373910293757747648３CA128

【図７】

【図7】

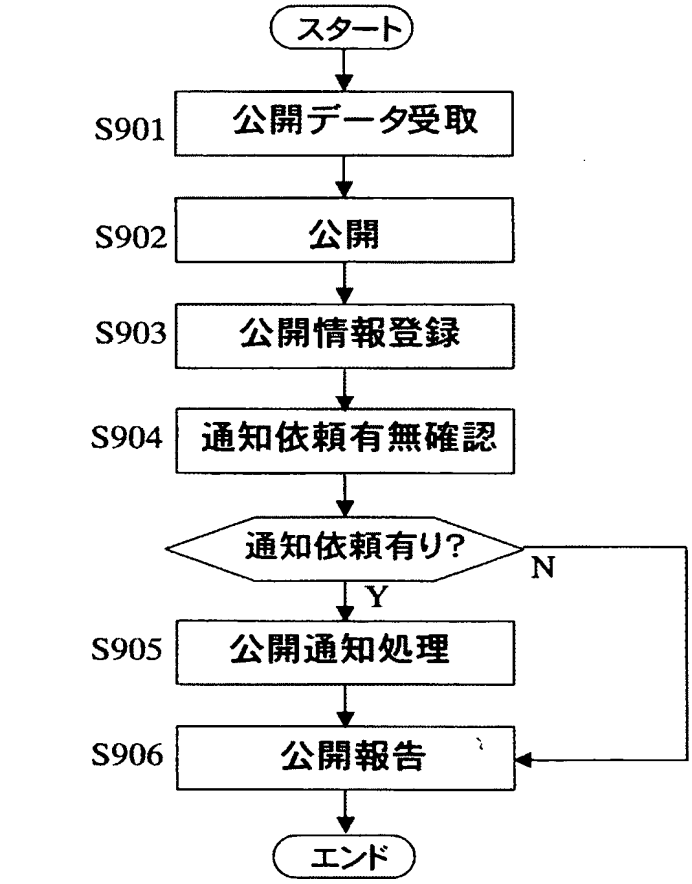

一般ユーザ側装置
「公開を依頼します」
署名記録
705
公開催促
706
「公開が滞っています」
701
公開サービス
702
公開催促サービス
「Bさんが公開したら知らせて下さい」
公開通知依頼
707
708
公開通知
「Bさんが公開しました」
「この署名を検証して下さい」
703
公開通知サービス
710
検証ログ
文書
署名
検証依頼
709
「検証結果です」
704
検証代行サービス
公開機関

【図８】


【図8】
802
記憶装置
807 送信プログラム
808 受信プログラム
809 公開プログラム
810 公開催促プログラム
811 公開通知プログラム
812 検証代行プログラム
813 履歴受信プログラム
814 公開データベース
815 公開通知依頼データベース
816 検証状況データベース
817 署名履歴保管領域
818 公開署名記録保管領域
819 検証代行依頼書保管領域
820 検証ログ保管領域
801 CPU
803 インターフェース
通信装置 804
入力装置 805
表示装置 806
ネットワークへ

【図９】

【図9】


公開処理
スタート
S901
公開データ受取
S902
公開
S903
公開情報登録
S904
通知依頼有無確認
通知依頼有り?
N
Y
S905
公開通知処理
S906
公開報告
エンド

【図１０】

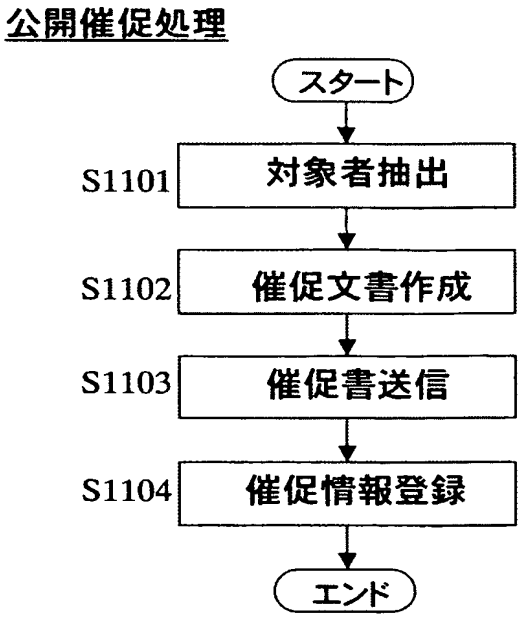
【図10】

1001 公開データベース

1002 ユーザ名	1003 公開ID	1004 署名番号	1005 公開場所	1006 公開日	1007 催促日	
ユーザA	000125	000002	http://www.X.co.jp/	2003.0710	－	1008
	000142	000032	http://www.X.co.jp/	2003.0802	－	1009
ユーザB	000225	000004	http://www.X.co.jp/	2003.0909	－	1010
ユーザC	000003	000003	http://www.X.co.jp/	2002.1104	2003.0618	1011
	000099	000155	http://www.X.co.jp/	2003.0620	2003.0729	1012
ユーザD	000090	000002	http://www.X.co.jp/	2003.0615	－	1013
	000118	000055	http://www.X.co.jp/	2003.0705	2003.0807	1014
	000148	000106	http://www.X.co.jp/	2003.0808	－	1015

【図１１】

【図11】

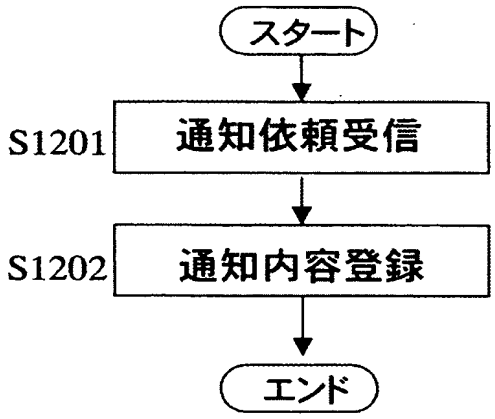


【図１２】

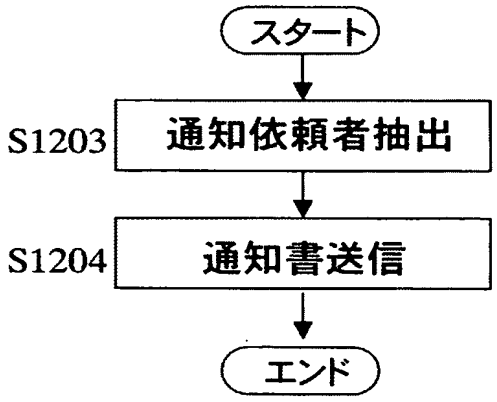
【図12】

公開通知処理

＜通知依頼受信処理＞



＜通知書送信処理＞



【図１３】

【図13】

1301 公開通知依頼データベース

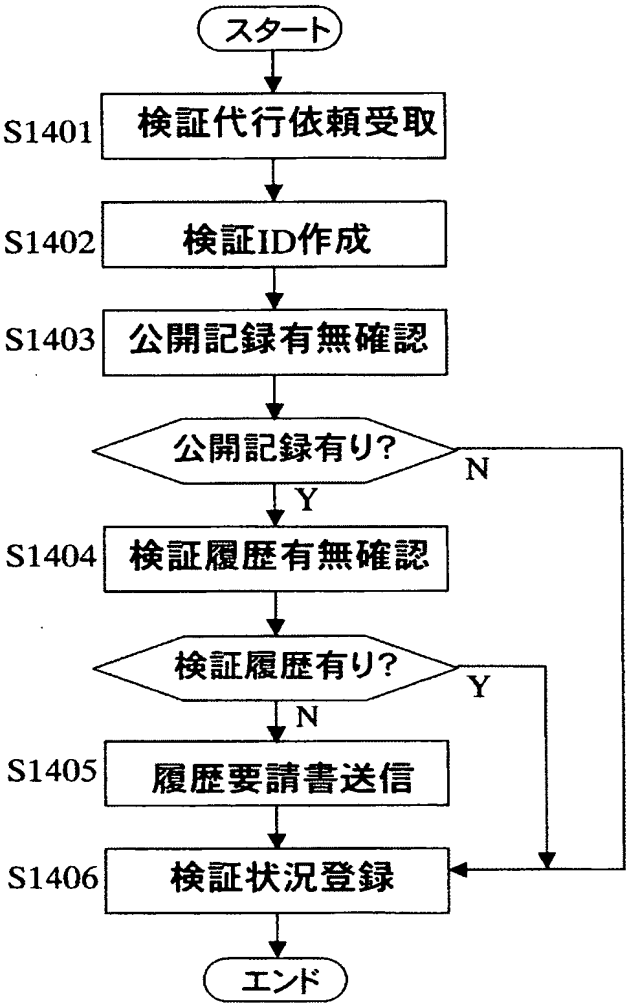
1302 被依頼ユーザ名	1303 依頼ユーザ名（メールアドレス）	1304 依頼日	1305 通知有無	
ユーザB	ユーザA（ユーザA@XX.co.jp）	2003.0710	未	1306
ユーザD	ユーザC（ユーザC@YY.co.jp）	2003.0511	2003.0522	1307
ユーザF	ユーザE（ユーザE@ZZ.co.jp）	2003.0330	未	1308

【図１４】

【図14】

検証代行サービス

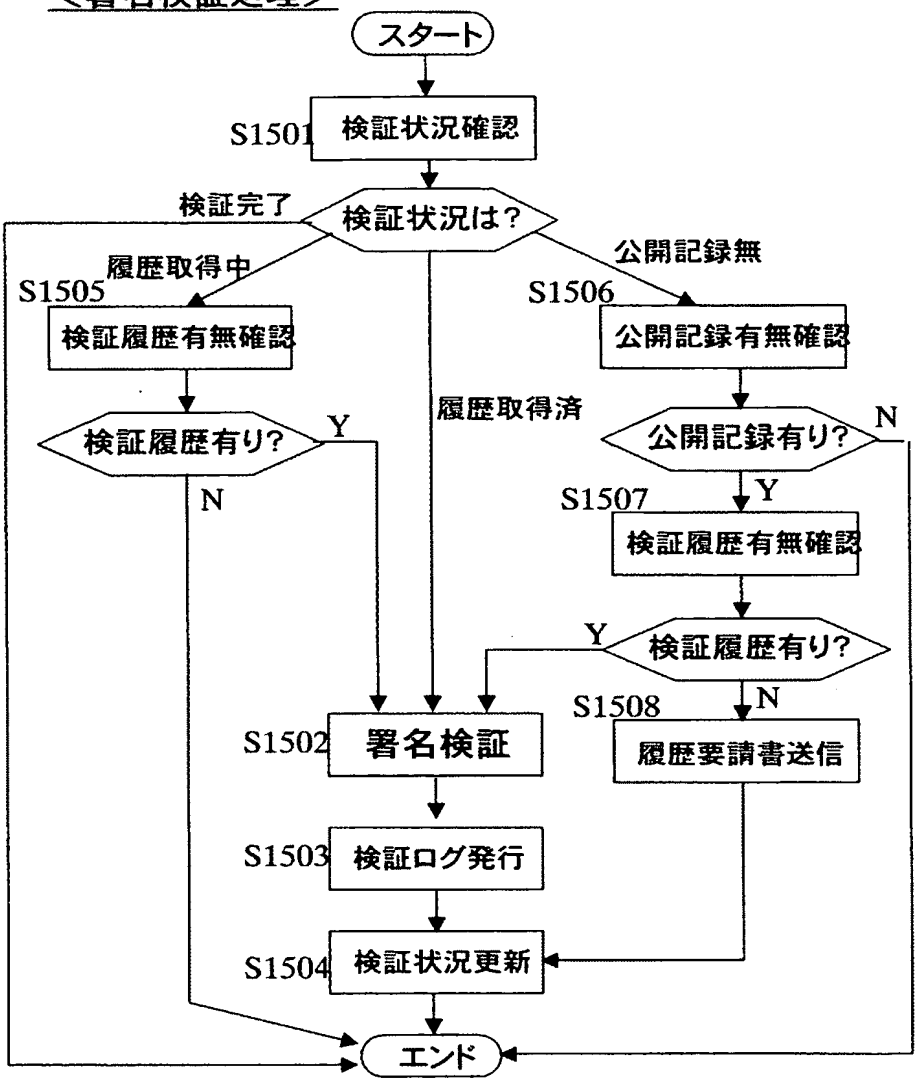
＜検証代行依頼書受信処理＞



【図１５】

検証代行サービス　【図15】

＜署名検証処理＞



【図１６】

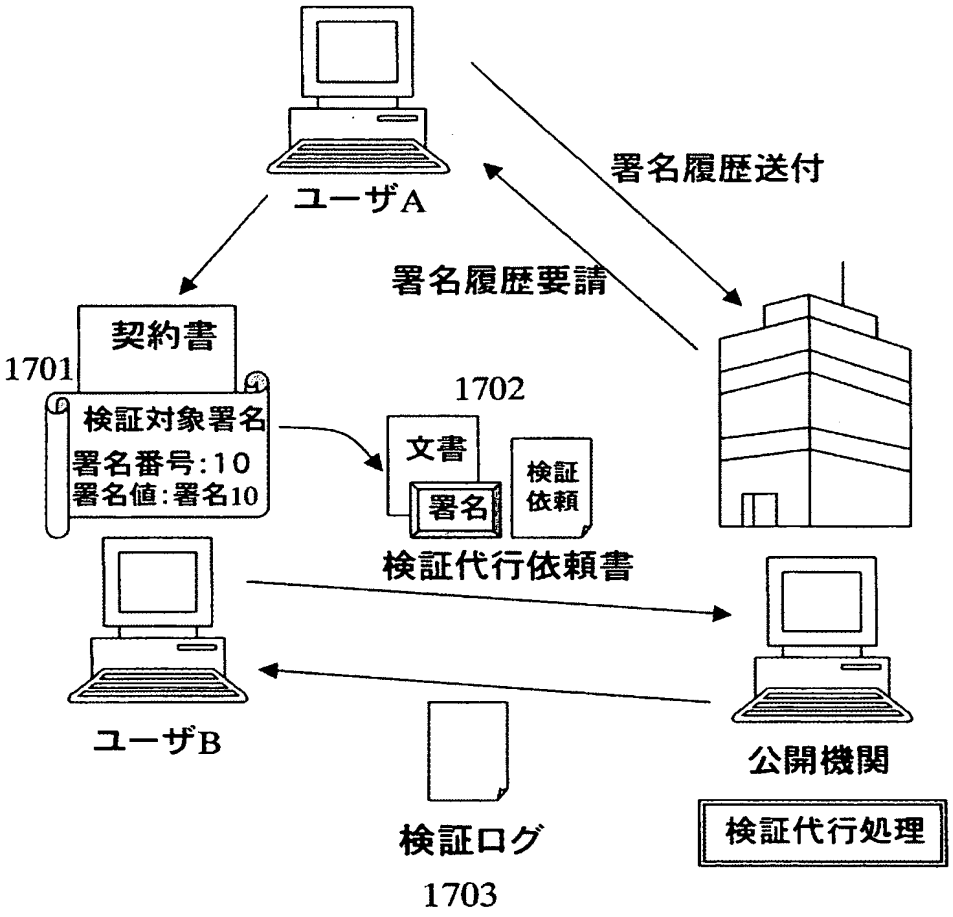
【図16】

1601 検証状況データベース

1602 検証ID	1603 依頼ユーザ名（メールアドレス）	1604 検証対象署名者（メールアドレス）	1605 公開ID	1606 依頼日	1607 検証状況	
000001	ユーザB（ユーザB@XX.co.jp）	ユーザA（ユーザA@XX.co.jp）	000142	2003.0910	履歴取得中	1608
000002	ユーザC（ユーザC@YY.co.jp）	ユーザE（ユーザE@YY.co.jp）	－	2003.0511	公開記録無	1609
000003	ユーザD（ユーザD@ZZ.co.jp）	ユーザF（ユーザF@ZZ.co.jp）	000065	2003.0830	履歴取得済	1610
000004	ユーザG（ユーザG@ZZ.co.jp）	ユーザH（ユーザH@KK.co.jp）	000102	2003.0420	検証完了	1611

【図１７】

【図17】


ユーザA
署名履歴送付
署名履歴要請
契約書
1701
検証対象署名
署名番号:10
署名値:署名10
1702
文書
署名
検証依頼
検証代行依頼書
ユーザB
公開機関
検証代行処理
検証ログ
1703

【書類名】要約書
【要約】
【課題】
ユーザ側装置に対して、検証した署名の証拠性を長期に渡って維持するための検証記録保存機能を提供する。また、公開機関側装置において、ユーザの署名の信頼性を保証するためのサービスを提供する。
【解決手段】
検証記録保存プログラムは、検証に使用した検証対象署名、署名履歴、預託公開署名記録を記録した検証ログを作成する。
また、公開機関側装置は、公開忘れの防止のための公開催促や、他のユーザの公開を知らせる公開通知や、ユーザに代わって検証の代行を行う検証代行など、信頼のある連鎖検証を確実に行え、かつユーザの利便性も考慮したサービスを提供する。
【選択図】　図７

認定・付加情報

特許出願の番号	特願２００４－０２８７９４
受付番号	５０４００１８５７５８
書類名	特許願
担当官	伊藤　雅美　　２１３２
作成日	平成１６年　２月　６日

＜認定情報・付加情報＞

【提出日】　平成16年 2月 5日

特願２００４－０２８７９４

出　願　人　履　歴　情　報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所